代数学 IB 試験

- 持ち込みは何でも可である。ただし、他人の迷惑になるもの、および通信機能をもつものを除く。
- 解答用紙には必ず学生番号と名前を記入すること。
- 解答用紙の裏面を用いてもよいが、その場合にはそれが分かるように明記すること。
- 言うまでもないことだが、数値的な答だけでは十分ではない。論理的な説明がもっと大事である。
- 成績は理学部 2 号棟 6F 数学コース掲示板において確認できるようにする。掲示があるまでは成績の照会等には応じられない。

問題 16.1. R,S は可換環であるとする。環準同型 $f : R \to S$ に対し、次の各問いに答えなさい。

(1) R の元 x, y の $R/\operatorname{Ker}(f)$ におけるクラスを $\bar{x}, \bar{y}$ と書いたとき、

$$f(x) = f(y) \Leftrightarrow \bar{x} = \bar{y}$$

であることを証明しなさい。

(2) $x \in R^\times$ ならば $f(x) \in S^\times$ であることを証明しなさい。

(3) R の元 x, y の最大公約数 $\gcd(x, y)$ の定義を述べなさい。(もちろん (必要ならば=貴方が本問の解答で使うならば) 約数や公約数の定義も書くこと。)

(4) R が PID で、$a \in \operatorname{Ker}(f)$ のとき、$\gcd(x, a) = 1$ なる任意の $x \in R$ に対し、 $f(x) \in S^\times$ であることを証明しなさい。

(5) (この小問は解いても加点されないが、参考までに) 小問 (2) の逆は必ずしも成り立たないことを示しなさい。

なお、必要に応じて、次の定理を用いて良い。定理の証明も込めた解答には加点する。

[定理] PID R の元 p, q が、$\gcd(p, q) = 1$ を満たすならば、ある $l, m \in R$ が存在して、

$$pl + qm = 1$$

を満たす。

[答]
(1) $x, y \in R$ に対して、

$$\begin{aligned} f(x) = f(y) &\Leftrightarrow f(x-y) = 0 && (f \text{ は準同型だから}) \\ &\Leftrightarrow f \in \mathrm{Ker}(f) && (\mathrm{Ker} \text{ の定義}) \\ &\Leftrightarrow \bar{f} = \bar{0} \in R/\mathrm{Ker}(f) && (\text{剰余環 } R/\mathrm{Ker}(f) \text{ における等号の定義}) \end{aligned}$$

(2) $x \in R^\times$ とする。ある $a \in R$ が存在して、$xa = 1$. 両辺を f で送ると、

$$f(x)f(a) = f(xa) = f(1) = 1.$$

よって、$f(x)$ は S 内で逆元 $f(a)$ が存在する。したがって、$f(x) \in S^\times$.
(3) R の元 x, y の最大公約数 $\gcd(x, y)$ の定義を述べなさい。
$*$ 約数の定義: a が b の約数 $\Leftrightarrow b \in aR$
$*$ 公約数の定義: c が a, b の公約数 $\Leftrightarrow c$ は a の約数で、かつ c は b の約数でもある。
$*$ 最大公約数の定義: d が x, y の最大公約数であるとは、次の 2 つが同時に満たされるときにいう。

(i.) d は x, y の公約数.
(ii.) d_1 が x, y の公約数なら、 d_1 は d の約数。

記号で、次のようにしても同じことである。
$*$ 最大公約数の定義 (記号版):

$$d = \gcd(x, y) \overset{\text{def}}{\Leftrightarrow} \begin{cases} x, y \in dR \\ x, y \in d_1 R \implies d \in d_1 R \end{cases}$$

(4) R は PID で、 $\gcd(x, a) = 1$ であるから、[定理] により、$\exists l, \exists m \in R$ が存在して、

$$lx + ma = 1$$

である。両辺を f で送ると、

$$f(l)f(x) + f(m)f(a) = f(1) = 1.$$

$a \in \mathrm{Ker}(f)$ であるから、$f(a) = 0$. ゆえに、 $f(l)f(x) = 1$ である。つまり $f(l)$ は $f(x)$ における S の逆元であって、$f(l) \in S^\times$.
(5) $R = \mathbb{Z}$ から $S = \mathbb{Z}/7\mathbb{Z}$ への環準同型 f を、

$$f(n) = \bar{n} = (n \text{ の } \mathbb{Z}/7\mathbb{Z} \text{ でのクラス})$$

で定義する。7 と 3 とは PID $\mathbb{Z}$ において互いに素であるから、全小問により、$f(3) = \bar{3}$ は $\mathbb{Z}/7\mathbb{Z}$ において可逆であることがわかるが、3 は $\mathbb{Z}$ において可逆ではない。

[定理] の証明。(簡略版; 詳細は各自考えよう。)
R のイデアル $I = Rp + Rq$ を考える。R は PID であるから、I はある一つの元 d で生成される。すなわち、

(★) $$I = Rd$$

(★) は 2 つのことを意味している。つまり、(「$\supset$」により、)

(あ) $$\exists l', m' \in R \text{ such that } l'p + m'q = d$$

(「$\subset$」により、)

(い) $$l \in dR, \qquad m \in dR$$

である。条件 (あ) から、$p, q \in d_1 R \implies d = lp + mq \in d_1 R$ がすぐにわかる。すなわち、d は 同伴を除いて 1 と等しい。言い換えると、d は可逆である。 (あ) の両辺に d^{-1} を掛けて、$l = l'd^{-1}, m = m'd^{-1}$ とおくことにより、求める式 $lp + mq = 1$ を得る。